Ms. Diane Honeycutt
National Institute of Standards and Technology
100 Bureau Drive, Stop 8930
Gaithersburg, MD 20899

Subject: Developing a Framework to Improve Critical Infrastructure Cybersecurity

ITT Exelis is a diversified, top-tier global aerospace, defense, information and technical services company that leverages a 50-year legacy of deep customer knowledge and technical expertise to deliver affordable, mission-critical solutions for global customers. We are a leader in communications, sensing and surveillance, critical networks, electronic warfare, navigation, air traffic solutions and information systems with growing positions in C4ISR, composite aerostructures, logistics and technical services. Headquartered in McLean, Va., the company employs about 19,900 people and generated 2012 sales of $5.5 billion.

Exelis is pleased to provide the following information in response to the National Institute of Standards and Technology's (NIST) Request for Information (RFI), Framework for Reducing Cyber Risks to Critical Infrastructure. The experience that Exelis brings to the table in the cybersecurity field can help assist NIST in its goal of developing a framework that includes and identifies common practices across sectors.

Exelis Current Risk Management Practices

Within Exelis, *organizational risk* is governed through formal risk assessments and audit processes by departments specifically structured for that purpose. *Cybersecurity risk* is governed through the Information Security Risk Management (ISRM) department, which is led by the Chief Information Security Officer (CISO). ISRM is aligned with the Exelis corporate headquarters and its members are geographically located at key sites throughout the organization. ISRM includes the functional areas of Risk and Governance, the Cyber Incident Response Center (CIRC), Awareness and Education, Cyber Operations and Architecture, and the Threat Intelligence Center.

Recognizing the importance of a security-aware culture, Exelis has developed a robust IT Security Awareness and Education Program. The program's objective is to provide Exelis employees with resources and tools they can use to help reduce the risk associated with being an end user, as well as strengthen their security acumen as the first and last line of defense. Supported by senior management, the essential components of this program are:

- Annual information security training
- Anti-phishing training and mock exercises
- Awareness newsletters
- Education website

In today's environment organizations must be able to convert vast amounts of threat data into applicable real time intelligence. As part of the ISRM department, Exelis has a Threat Intelligence Center that analyzes multiple government and private sector threat feeds transforming the information into actionable intelligence. This intelligence is then used by Exelis to accomplish its strategic cybersecurity goal of fundamentally improving the overall IT Security posture. The practice of *Threat Intelligence and*

Threat Modeling is growing throughout many sectors and should be considered for inclusion in the NIST Cybersecurity Framework.

A vital component of information sharing is sharing the information in a secure and timely manner. To accomplish this, Exelis regularly reports to the Defense Security Service (DSS), Federal Bureau of Investigation (FBI), and the Defense Industrial Base (DIB) Information Assurance Working Group. At times, the reporting process has been labor-intensive, particularly when Exelis is required to report to more than one agency for a given incident. However, the value added from information sharing across industry practitioners has proven to be instrumental in our cybersecurity investigations. Moving forward, NIST should work to standardize a framework for information sharing and intelligence gathering. The intelligence and information currently disseminated from many government agencies is not standard making it difficult for organizations to process and apply it in a timely fashion. Standardizing and normalizing the information will allow the organization to automate portions of the threat intelligence cycle, such as:

- Implementing network blocks
- Creating customized scans
- Attribution
- Historical trending and forecasting

Exelis Use of Frameworks, Standards, Guidelines, and Best Practices

The framework for the Exelis IT Security policy is risk-based. It is derived from the ISO 27002 and various NIST 800 series documents. Other standards being explored include OWASP (Open Web Application Security Project) Top Ten and Development Guide, SANS Critical Top Twenty, as well as various Microsoft best practices and security standards. To achieve our security objectives and drive risk down, the Exelis IT Security Policy covers the following areas:

- IT Security Risk Assessments
- Systems Security Control Requirements
- IT Security and Architecture Standards
- Systems Security Review
- Security Monitoring
- Incident Handling and Response

ITT Exelis appreciates the opportunity to share information and collaborate with NIST in support of the Cybersecurity Framework Development efforts. We are pleased to share our industry perspectives and look forward to continuing our support to NIST in the future.